REMARKS

Claims 1-5, 9-22, 24-29, and 32 are currently pending in the subject application and are presently under consideration. Claims 1, 2, 4, 5, 9-15, 17, 18-25, 27, and 28 have been amended; claim 23 has been canceled; and claim 32 is new as shown on pp. 2-7 of the Reply. Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Objection to Claims 21 and 23

Claims 21 and 23 stand objected to for the following informalities. Claim 21 is objected to because "extended security protocol" is not disclosed in claim 20, upon which claim 21 depends. Additionally, claim 23 is objected to because "path component" is not disclosed in claim 20, upon which claim 23 depends. Claim 21 has been amended, and claim 23 has been canceled to cure the minor informalities. Accordingly, the withdrawal of the objection is respectfully requested.

II. Rejection of Claims 1-5 and 9-24 Under 35 U.S.C. §103(a)

Claims 1-5 and 9-24 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Swales (US 6,760,782) (hereinafter "Swales") in view of Branstad, *et al.* (US 6,842,860) (hereinafter "Branstad"). Withdrawal of this rejection is respectfully requested for the following reasons. Swales and Branstad, alone or in combination, fail to disclose or suggest each and every aspect of the claimed subject matter.

Applicants' claimed subject matter relates to extending factory protocols used in the network communication of an automation system. This extension of the factory protocol includes security parameters and enables secure communications between automation assets, including communication between an automation control device and a remote automation control device across a network communication channels. To this end, claim 1 recites in part: *an automation asset operatively coupled to a network communication channel,* ***an automation asset comprises at least an automation control device*** *and implements the following: an extensible factory protocol to transport data between the automation asset and an automation asset on a remote network communication channel,* ***the extensible factory protocol is a control-specific transport mechanism for data exchange between automation assets that encodes at least one***

security field within the extensible factory protocol to exchange data with the remote automation asset. Swales or Branstad, alone or in combination, fail to disclose or suggest such aspects.

Swales generally relates to the transfer of real time control data with guaranteed delivery times between devices on a general purpose network and an industrial control system. Swales discusses that industrial automation systems often employ real-time solutions through at least three layers or levels. *See* Swales col. 1 lines 21-43. Swales discusses that the highest level is the conventional data processing communication networks such as the Internet and World Wide Web, *e.g.* general purpose networks. *See* Swales col. 1 lines 44-60. The lowest level is the specialized moving bus level, or the level that allows the control devices to exchange information with sensors and actuators. *See* Swales col. 1 line 44 – col. 2 line 6. The middle level is a fieldbus layer that allows for the supervision and updating of the control devices. *See* Swales col. 2 lines 7-16. The goal of Swales is to allow for the use of a general purpose network, *e.g.* Ethernet, Token Ring, or ATM, on all three levels of an automation control system so that the automation devices use commercial network techniques. *See* Swales col. 2 lines 17-23.

In Swales, leveraging the same level protocol, a protocol such as TCP/IP that is related to commercial techniques, introduces a level of interruption between the real-time communication demand of industrial control system (*e.g.* deterministic network connection) and the on-demand traffic from the general purpose network (*e.g.* non-deterministic network communication). A web site provided by a web server that plugs directly into the backplane of the control system to provide access for on-demand traffic from the Internet. *See* Swales col. 4 lines 32-60. To maintain the deterministic aspect of the industrial control system, Swales introduces a proxy server to interface the on-demand traffic from the web server. *See* Swales col. 2 lines 39-59. The proxy server takes the role of a TCP/IP router to provide security as a firewall and limit network throughput as the interface. *See* Swales col. 2 lines 39-59. Swales emphasizes that this proxy server or firewall provides the "necessary security" from outside access to the industrial control system. *See e.g.* Swales col. 4 lines 37-38; col. 9 64-67; col. 10 lines 60-62. This proxy server throttles requests from the on-demand (non-deterministic) portion of the network so as not to disturb the real-time communications occurring within the real-time portion of the network. *See* Swales col. 2 lines 39-59; col. 10 lines 24-40. Swales discusses the use of MODBUS as an

application protocol for the backplane of the system. *See* Swales col. 10 lines 64-66. However, Swales fails to disclose or suggest the aforementioned aspects of subject claim 1. Branstad fails to cure the deficiencies of Swales.

Branstad generally relates to providing an authentication system that implements a strength performance tradeoff. *See* Branstad col. 1 lines 59-61. Branstad discloses a network authentication system designed to adaptively adjust its authentication strength and speed to meet current needs based on considerations such as security policy, observed authentication error rates, alarms from host or network defenses, and processor loading. *See* Branstad col. 4, lines 2. More particularly, Branstad discusses the use of an adaptive cryptographically synchronized authentication (ASCA) system to implement this strength performance tradeoff. *See* Branstad col. 4 lines 13-24. This ASCA system determines what level security mechanism should be implemented for data exchanged between nodes sharing a given security association. *See* Branstad col. 4 lines 13-24. Branstad further describes implementing its strength performance system through the openly developed network security software IPsec. *See e.g.* Branstad col. 9 lines 23-30. However, Branstad fails to cure the deficiencies of Swales.

As discussed above, subject claim 1 recites: *the extensible factory protocol is a control-specific transport mechanism for data exchange between automation assets that encodes at least one security field within the extensible factory protocol to exchange data with the remote automation asset*. In contrast, Swales merely relates to opening communication access to a deterministic industrial control system *via* TCP/IP through the integration of a web server and proxy or firewall. Thus for a user external to the industrial control system or network of Swales, the user must access the system through a web server. All on-demand user requests or non-deterministic communications are throttled through the proxy or firewall on the web server attached to the industrial control network. After the on-demand requests are intercepted by this proxy server, and the proxy server then makes a request when it will not disturb the deterministic aspect of the control system. Therefore, Swales does not implement an extensible factory protocol that is a control-specific transport mechanism for data exchange between an automation asset and a remote automation asset as contemplated in subject claim 1 because Swales limits its communication across the network through a non-control-specific TCP/IP protocol. Swales discusses the use of MODBUS as the application control protocol within the industrial control system, but does not disclose or suggest the extensibility of this particular protocol for data

exchange to a remote automation asset. Thus Swales fails to disclose or suggest each and every aspect of subject claim 1.

Branstad fails to cure the deficiencies of Swales because Branstad only relates to implementing a system that has different security mechanism levels based on desired performance. The Swales system is implemented with the IPsec security package, which as the Examiner asserts in the Office Action, is part of the Internet Protocol suite TCP/IP. *See* Office Action p. 4. Thus, to begin, IPsec is not an extensible factory protocol because it is not a *control-specific* transport mechanism for *data exchange between automation assets*. Moreover, the IPsec security package relates to a form of encapsulating the protocol rather than being encoded *within* the protocol. In general, IPsec relates to establishing a secure channel *(e.g.* a tunnel) that is configured between two endpoints to enable information to be securely exchanged between the endpoints. This "tunnel" is when an inner protocol is transported as the payload of another outer protocol. This encapsulation process is typically accomplished by attaching the outer protocol "header" to the inner protocol, thus creating a new, larger protocol. In contrast, the extensible factory protocol in the subject claim *encodes at least one security field* ***within*** *the extensible factory protocol* rather than adding on a new header to make a new, larger, and different protocol. To this end, it is respectfully submitted that Branstad fails to cure the aforementioned deficiencies of Swales. In view of the foregoing, it is respectfully requested that the rejection of claim 1 be withdrawn.

Moreover, subject claim 1 recites that: *an automation asset comprises at least an automation control device*. Thus, taken in conjunction with the aforementioned aspects, wherein the *extensible factory protocol... that encodes at least one security field within the extensible factory protocol ... to exchange data with the remote automation asset*, it is readily apparent that Swales fails to disclose each and every aspect of the subject claim. Swales merely allows external access to the deterministic system – that is if the access does not impact the real-time communications of the Swales control system – *via* a communication generated by the proxy server. It must be appreciated that the inherent nature of a proxy server intercepts requests from the web server and will complete the request on behalf of the web server. Thus, because any remote communication Swales is through a web server *via* the proxy on behalf of the web server, Swales fails to disclose or suggest that the data exchange across the general purpose network and the industrial control system is between an automation asset and a remote automation asset

wherein the automation asset comprises at least an automation control device. Again, Branstad fails to cure the aforementioned deficiencies because Branstad does not relate to data exchange between an automation asset and a remote automation asset across a network communication channel. To this end, it is respectfully submitted that Swales and Branstad, alone or in combination, fail to disclose or suggest each and every aspect of subject claim 1.

In view of the foregoing, it is respectfully submitted that Swales and Branstad, alone or in combination, fail to disclose or suggest each and every aspect of claim 1. It is respectfully requested that the rejection of claim 1, and claims 2-5 and 9-16 that depend therefrom, be withdrawn.

With respect to claims 13, 14, 16, 18, and 19, it is admitted in the Office Action that neither Swales nor Branstad specifically disclose each and every aspect of the subject claims. *See* Office Action p. 7. In particular, claim 13 recites: *the factory protocol is associated with a protocol supporting at least one of: a Temporal Key Interchange Protocol (TKIP) or a wireless protocol*. Claim 14 recites: *the protocol employing at least one of: an Elliptical function, an Aziz/Diffie Protocol, a Kerberos protocol, a Beller-Yacobi Protocol, an Extensible authentication protocol (EAP), an MSR+DH protocol, a Future Public Land Mobile Telecommunication Systems Wireless Protocols (FPLMTS), a Beller-Chang-Yacobi Protocol, a Diffie-Hellman Key Exchange, a Parks Protocol, an ASPeCT Protocol, a TMN Protocol, RADIUS, Groupe Special Mobile (GSM) protocol, or a Cellular Digital Packet Data (CDPD) protocol*. Moreover, claim 16 recites: *a security field to limit access based upon line of sight parameters*. Amended claim 18 recites: *incorporating a TKIP protocol in an automation protocol*. Although claim 18 is amended, claim 18 still recites the wireless security protocol of TKIP which is an admitted deficiency of Swales and Branstad. Lastly, claim 19 recites: *utilizing at least one of: a Temporal Key Interchange Protocol (TKIP) or an Elliptical function in the wireless security protocol*. It is admitted in the Office Action that Swales and Branstad fail to disclose such aforementioned aspects. *See* Office Action dated October 1, 2008 (hereinafter "Office Action") p.7. To cure such deficiencies, it appears that the Examiner has taken Official Notice with respect to these claims by asserting that "[i]t is commonly known to one of ordinary skill in the art that various wireless, including those using line of sight parameters, and communication protocols can be used within and automated factory network." *See* Office Action p. 7.

Applicants' representative respectfully disagrees with the assertion that the aforementioned statements are well known and requests that the Examiner cite a reference in support of his position pursuant to MPEP §2144.03 if such rejection of these claims is to be maintained. Official Notice unsupported by documentary evidence should only be taken by the Examiner where the facts asserted to be well-known, or to be common knowledge in the art are capable of instant and unquestionable demonstration as being well-known. Furthermore, the facts asserted to be well known must be asserted as well known *at the time the invention is made*. If, as asserted in the Office Action that it would be obvious for Swales and Branstad to be adaptable and implemented on multiple network protocols, then it is not clear why there is not even a contemplation or suggestion of any of the plurality of protocols recited in the subject claims, including the implementation of wireless systems, wireless protocols, or line of sight network security. Furthermore, the lack of contemplation in the cited art suggests a contrary position taken in the Official Notice. The lack of contemplation implies that it was *not* well known in the art *at the time the invention was made* to utilize the above mentioned in an *automation security system* as recited in claim 1 or the *method to facilitate factory automation security* as recited in claim 17, upon which claims 13, 14, 16, 18, and 19 depend. To this end, it is respectfully submitted that Official Notice fails to cure the admitted deficiencies of Swales and Branstad. It is respectfully requested that the rejection of claims 13, 14, 16, 18, and 19 be withdrawn.

Applicants' claimed subject matter further relates to implementing wireless security protocols for communication between automation devices in the automation system. In particular, independent claim 17 recites: ***adapting a wireless security protocol for communication between automation devices of the industrial automation system by lowering the security requirements if real-time performance is required***. It is admitted in the Office Action with respect to claim 13 that neither Swales nor Branstad discloses at least *a wireless protocol*. It follows that if Swales or Branstad each fail to disclose a wireless protocol, Swales and Branstad, alone or in combination, fail to disclose or suggest a wireless security protocol and thusly the aforementioned aspects. To this end, it is readily apparent that Swales and Branstad fail to disclose or suggest each and every aspect of subject claim 17. Withdrawal of the rejection of claim 17, and claims 18 and 19 that depend therefrom, is respectfully requested.

Moreover, applicants' claimed subject matter relates to a method to facilitate automation network security using either a heavyweight encryption mechanism or a lightweight encryption

mechanism based on the demand for performance. To this end, claim 20 recites: ***establishing a communications session with a remote automation control device across an automation control network via a heavyweight encryption mechanism in a security protoco****l employed in the communication session if real-time communications is not needed; and* ***exchanging data between the automation control device and the remote automation control device in accordance with real-time communications via a lightweight encryption mechanism in the security protocol*** *that induces minimal impact on system performance if real-time communication is needed.* Swales and Branstad, taken together or taken separate, fail to disclose or suggest such aspects. As discussed above, the communication from the general purpose network to the industrial control system of Swales is through a web server and proxy or firewall. The communication is not between an automation control device and a remote automation control device through a security protocol employed in the communication session as recited in subject claim 20, because the Swales proxy places the on-demand communication requests on behalf of requests coming through the web server. For this reason alone, Swales fails to disclose or suggest all aspects of the subject claim. Branstad does not relate to automation control networks and fails to disclose establishing communication sessions between an automation control device and remote automation control device across an automation control network. Thus, alone or in combination, Swales and Branstad fail to disclose or suggest the aforementioned aspects of claim 20, and withdrawal of the rejection is respectfully requested.

Moreover with respect to claim 20, Swales does disclose real-time communications *within* the industrial control system, but because any remote network Swales communication is intercepted by the proxy so as to not interrupt the real-time communication in the control system, Swales does not disclose or suggest exchanging data between the automation control device *and the remote automation control device in accordance with real-time communications* as recited in claim 20. Additionally, Branstad fails to relate to automation control devices and fails to cure this deficiency.

To this end, Swales and Branstad, alone or in combination, fail to disclose or suggest each and every aspect of claim 20. It is respectfully requested that the rejection of claim 20 be withdrawn.

Furthermore, claim 24 recites in part: ***means for encoding a security component within a factory protocol, the factory protocol is specifically adapted for data exchange between***

automation assets in a control domain *and includes at least one of a security parameter or a performance parameter that is determined by at least one automation asset;* ***means for transmitting the security component and the factory protocol across a network between an automation asset in the control domain and an automation asset remote to the domain***. Swales and Branstad fail to disclose or suggest such aspects when taken alone or taken in combination. Similar to the discussion above with respect to claims 1 and 20, Swales interposes a web server and proxy or firewall between communications from user terminals or computers or alarm systems in the general purpose network trying to make an on-demand request in the industrial control system. Thus, in addition to Swales failing to disclose or suggest that transmissions between an automation asset in the control domain and an automation asset remote to the domain, Swales further fails to transmit the factory protocol *specifically adapted for data exchange between automation assets* because it uses the TCP/IP proxy that is not specifically adapted for data exchange between automation assets. Additionally, Branstad fails to relate to communication between automated control devices and fails to cure such deficiency. Moreover, as discussed above, Branstad relates to an IPsec which creates larger protocols by appending headers to the outside of other protocols. Branstad thus further fails to relate to *means for encoding a security component within a factory protocol.* Therefore, it is respectfully submitted that Swales and Branstad, alone or in combination, fail to disclose or suggest each and every aspect of subject claim 24. It is respectfully requested that the rejection of claim 24 be withdrawn.

In view of the foregoing, it is Swales and Branstad, alone or in combination, fail to disclose or suggest all aspects of the subject claims. Therefore, it is respectfully requested that the rejection of claims 1-5, 9-22, and 24 be withdrawn. The rejection of claim 23 is moot because the claim has been canceled.

III. Rejection of Claims 25-29 Under 35 U.S.C. §103(a)

Claims 25-29 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Swales in view of Branstad, and further in view of Bridges, *et al.* ("AI Techniques Applied to High Performance Computing Intrusion Detection") (hereinafter "Bridges"). It is respectfully submitted that this rejection be withdrawn for the following reasons. Swales, Branstad, and

Bridges, alone or in combination fail to disclose or suggest each and every aspect of the subject claims.

Applicants' claimed subject matter relates to an automation security system that implements an extensible factory protocol to facilitate data exchange between control devices and includes an intrusion detection system adapted to the factory protocol to detect network attacks directed at the control device. To this end, claim 25 recites in part: ***a control device that utilizes an extensible factory protocol, the extensible factory protocol is implemented for data exchange between control devices across more than one communication network***. Swales, Branstad, and Bridges, alone or in combination fail to disclose or suggest such aspects. As discussed above. Swales merely relates to the use of a TCP/IP protocol to facilitate the exchange of data across the general purpose network and the industrial control system network. However, the TCP/IP protocol is not an *extensible factory protocol is implemented for data exchange between control devices*, and Swales fails to disclose or suggest the use of the TCP/IP protocol for *data exchange between control devices across more than one communication network*. To this end, it is readily apparent that Swales fails to disclose all aspects of claim 25. Branstad fails to cure Swales because Branstad fails to relate to data exchange between control devices. Lastly, Bridges further fails to disclose or suggest such aspects. Bridges merely relates to a prototype intrusion detection system that uses specific artificial intelligence approaches to intrusion detection. To this end, Bridges fails to cure the aforementioned deficiencies of Swales and Branstad, and it is respectfully requested that the rejection of claim 25, and the claims 26 and 27 which depend upon claim 25, be withdrawn.

Lastly, claim 28 relates to a methodology for detecting security violations by monitoring the industrial network protocol. To this end, claim 28 recites in part: *monitoring the industrial network protocol for an attack via the intrusion detection technology,* ***the monitoring is conducted at a first security level if real-time performance is requested between automation devices employing the industrial network protocol in remote networks****, and a second security level if real-time performance is not requested, the first security level is lower than the second.* Swales, Branstad, and Bridges, taken alone or taken together, fail to disclose or suggest such aspects. As discussed above, Swales relates to remote networks but not to an industrial protocol across the networks because Swales implements TCP/IP to communicate between the general purpose network and the industrial control network. Swales also only relates to real-time

performance within the industrial control network. The on-demand (non-deterministic) requests are not real time because they are governed and delayed by the Swales proxy. Thus, Swales fails to disclose automation devices interacting between automation devices in the remote networks, or in other words, *real-time performance is requested between automation devices employing the industrial network protocol in remote networks*. Branstad still fails to cure the deficiency of Swales because Branstad fails to relate to industrial network protocols and further fails to relate to control device performance from control devices in remote networks. Bridges merely relates to intrusion detection and fails to cure the aforementioned deficiencies. To this end, it is readily apparent that the cited art of record in this rejection fails to disclose or suggest all aspects of subject claim 28. Withdrawal of the rejection of claim 28, and claim 29 which depends upon claim 28, is respectfully requested.

In view of the foregoing, it is respectfully submitted that Swales, Branstad, and Bridges, alone or in combination, fail to disclose or suggest each and every aspect of claims 25 and 28, upon which claims 26-27 and 29 depend. Therefore, it is respectfully requested that this rejection be withdrawn.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [ALBRP303USB].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

AMIN, TUROCY & CALVIN, LLP

/Adam P. Slepecky/
Adam P. Slepecky
Reg. No. 61,170

AMIN, TUROCY & CALVIN, LLP
127 Public Square
57TH Floor, Key Tower
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731